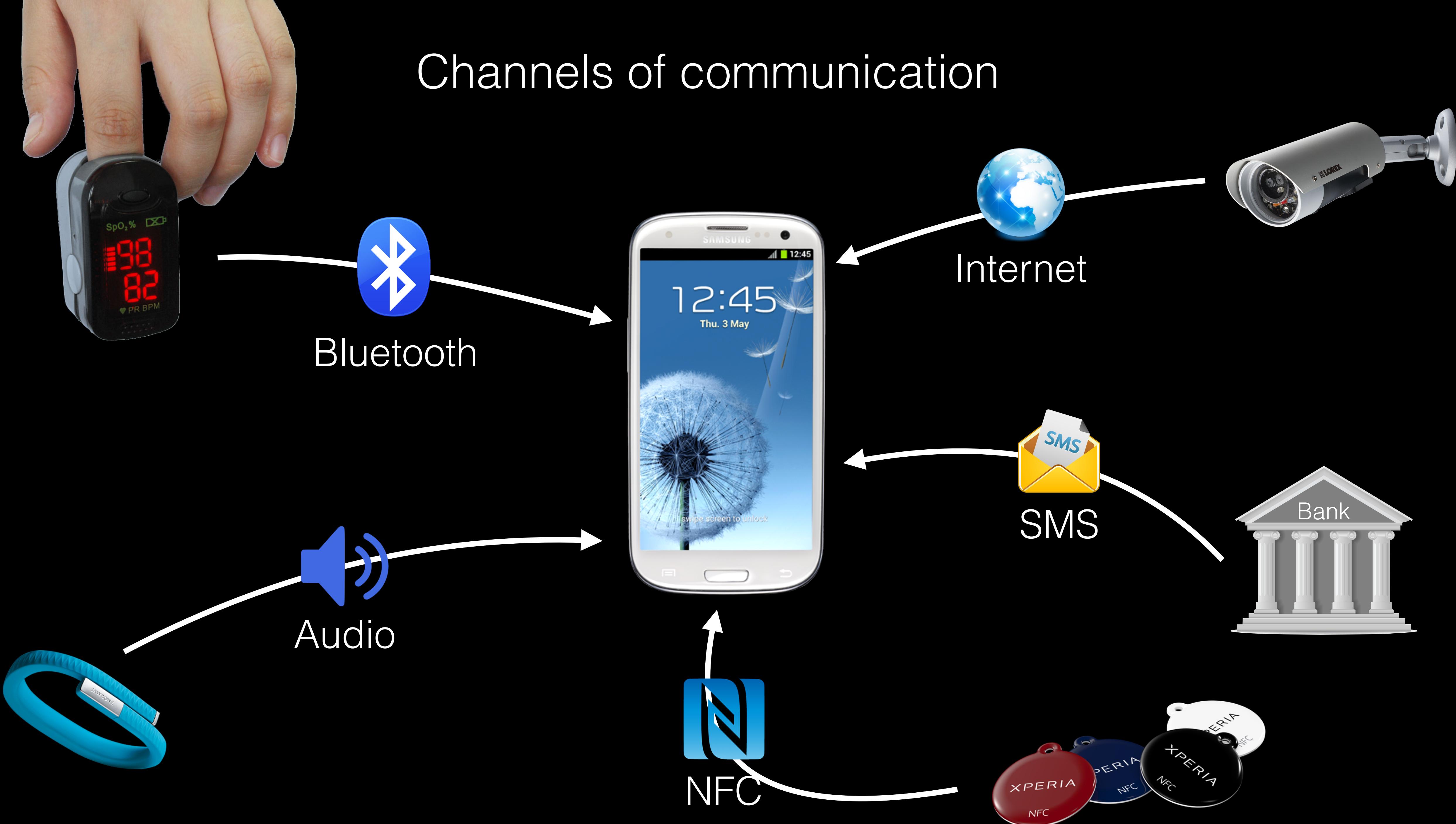


What's in Your Dongle and Bank Account? Mandatory and Discretionary Protection of Android External Resources

Soteris Demetriou ♦ ▼ , Xiaoyong Zhou ♦ ▼ , Muhammad Naveed ♦ ,
Yeonjoon Lee ♦ , Kan Yuan ♦ , XiaoFeng Wang ♦ , Carl A. Gunter ♦



Channels of communication

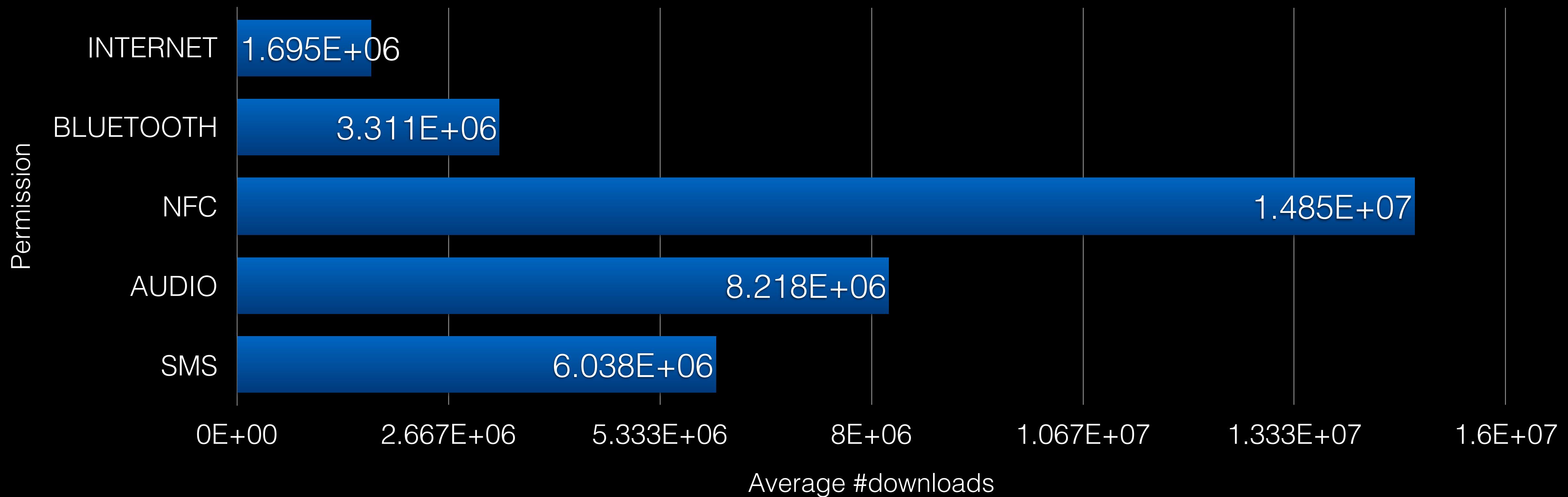


Channels of communication

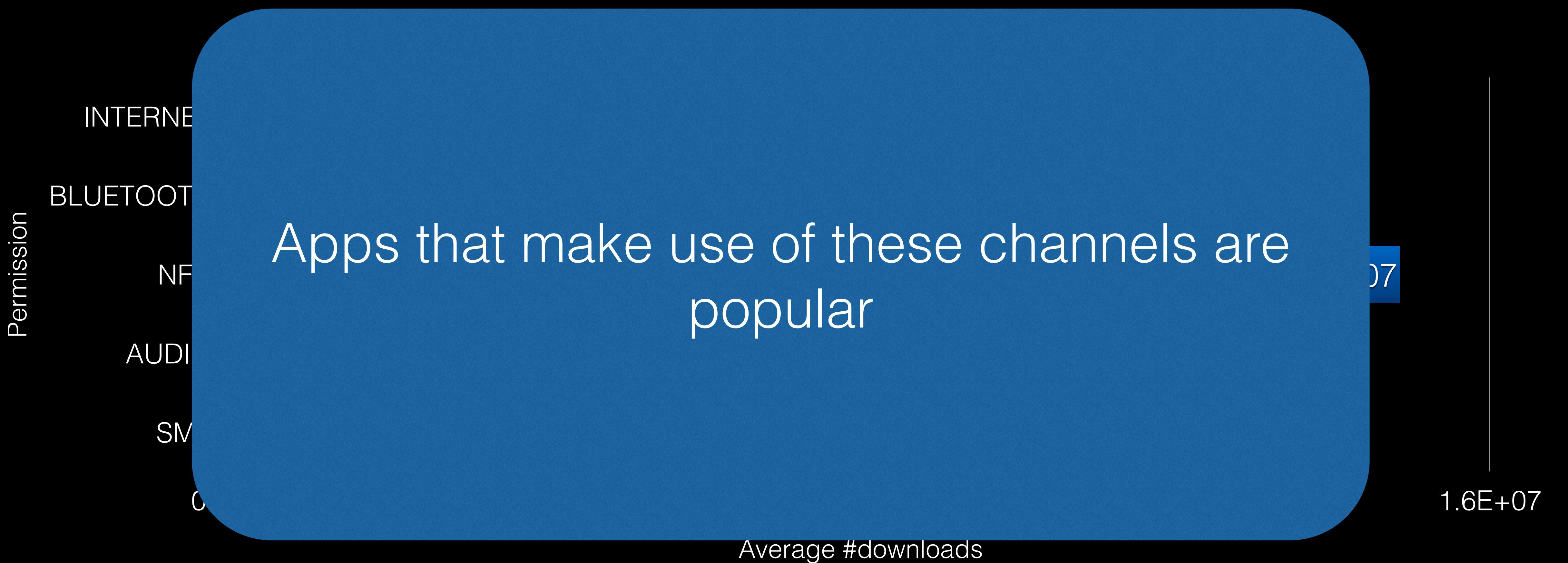
These channels often carry sensitive information



Channel Use



Channel Use



Problem Statement



Approach

Approach

OS-level Access Control: flexible and uniform

- Permissions: user DAC
- SELinux: admin MAC

Approach

OS-level Access Control: flexible and uniform

- ~~Permissions: user DAC~~

coarse-grained VS

permission
bloat

- SELinux: admin MAC

SELinux



SELinux

User Policies:

- Personal Resource Management

Vendor / Admin Policies:

- BYOD
- Mobile App Management (MAM)
- Mobile Device Management (MDM)

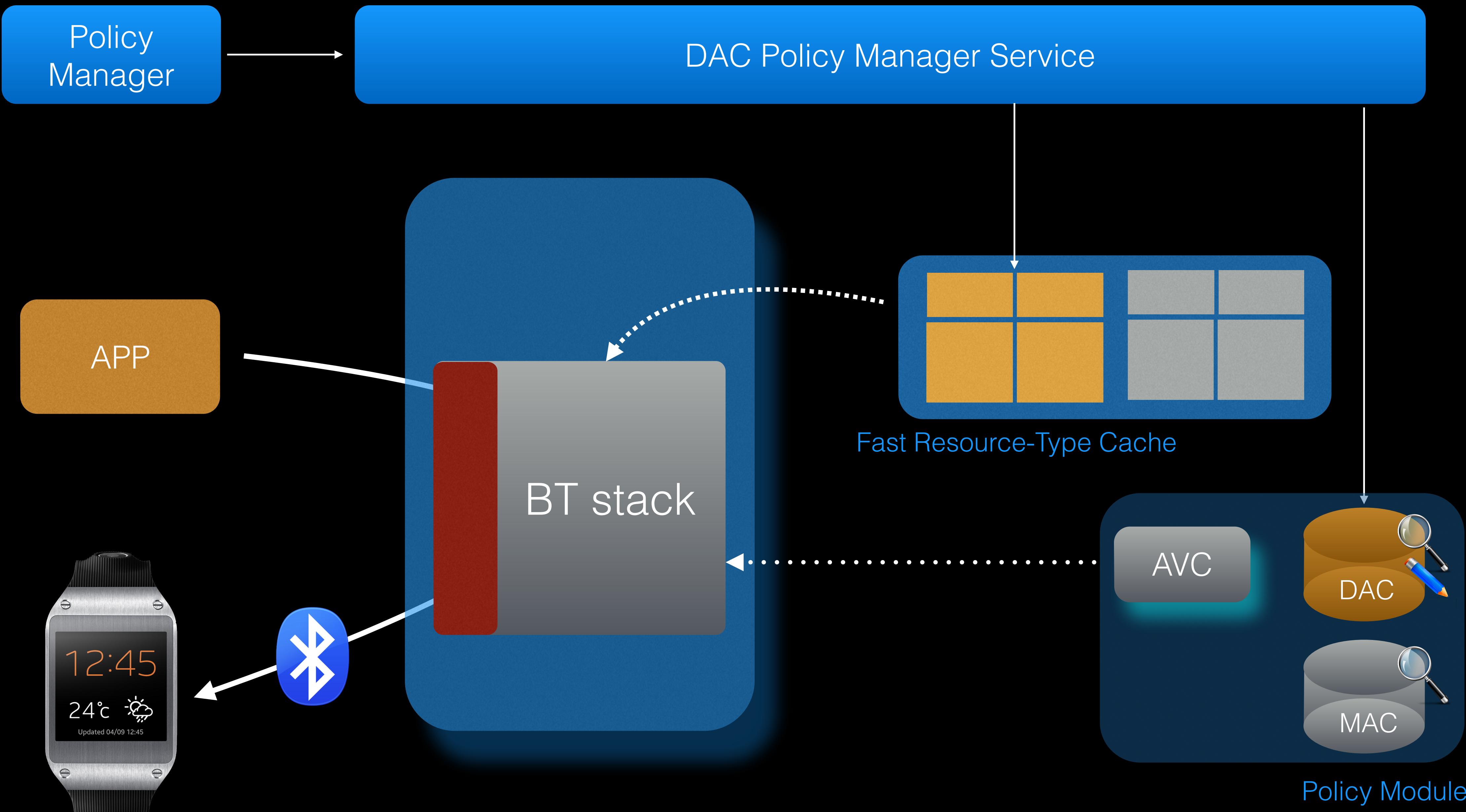
DAC | MAC

The background of the slide is a slightly out-of-focus photograph of two seals resting on a light-colored, rocky or sandy beach. The sky above is a clear, pale blue.

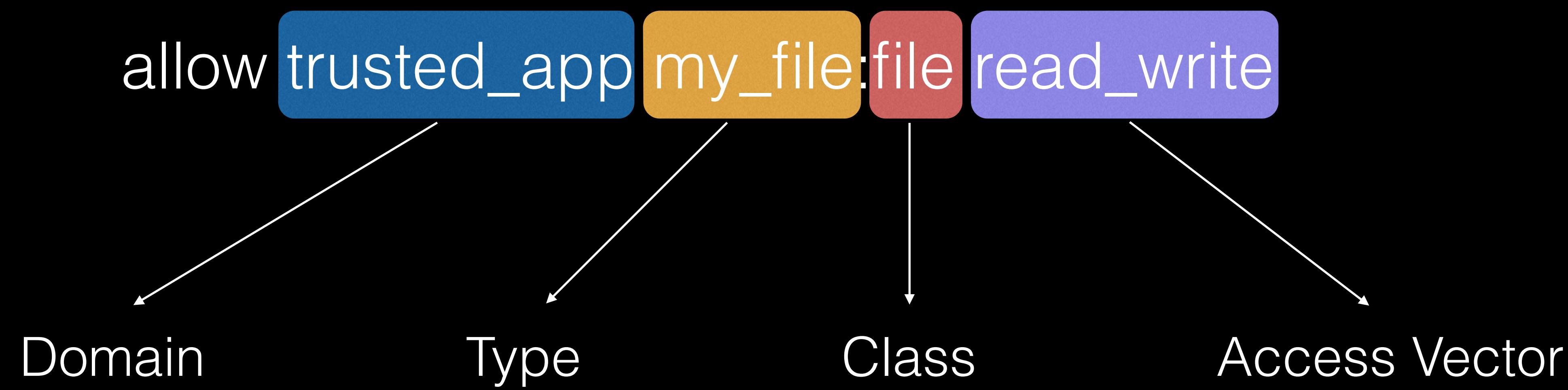
SEACAT

Security Enhanced Android Channel Access Control

SEACAT Overview

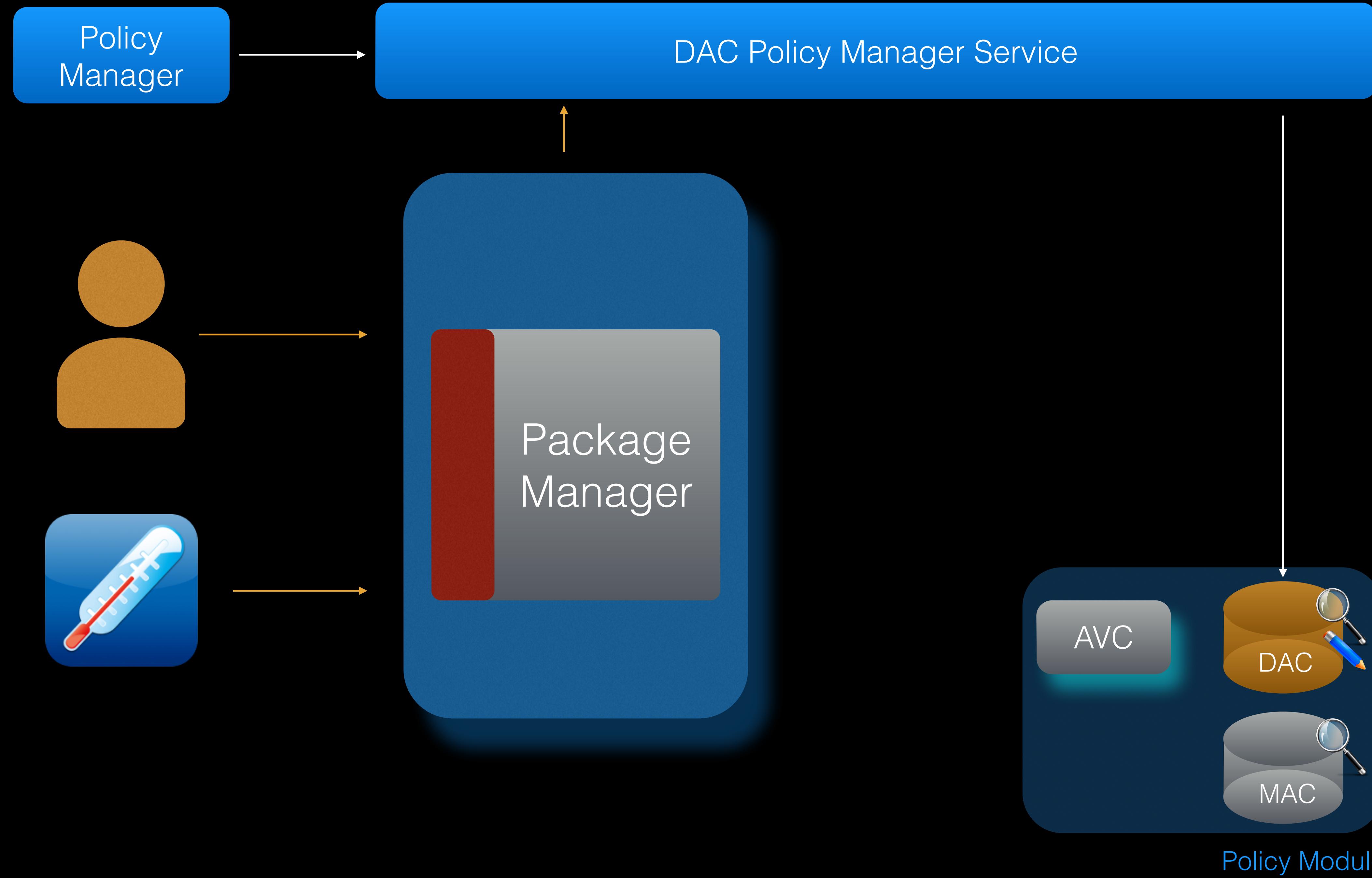


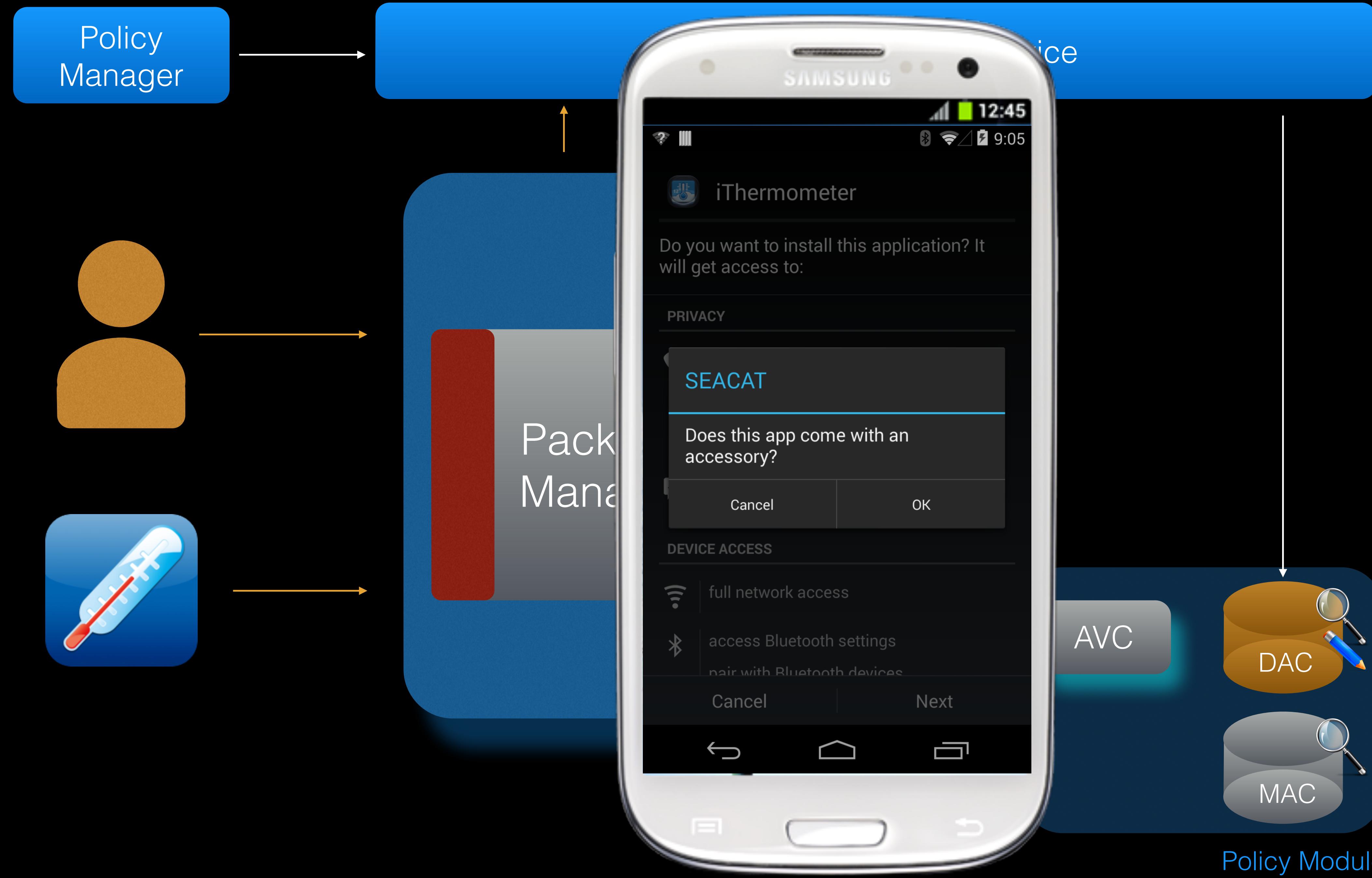
SELinux rule



Assigning Apps to Domains

```
allow trusted_app my_file:file read_write
```



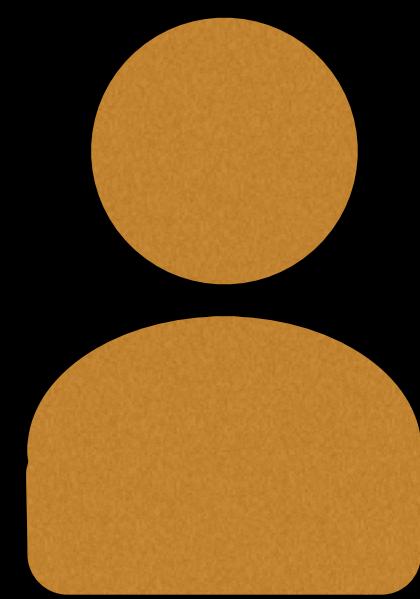


Assigning External Resources to Types

```
allow trusted_app my_file:file read_write
```

Policy
Manager

DAC Policy Manager Service



Bluetooth



Fast Resource-Type Cache

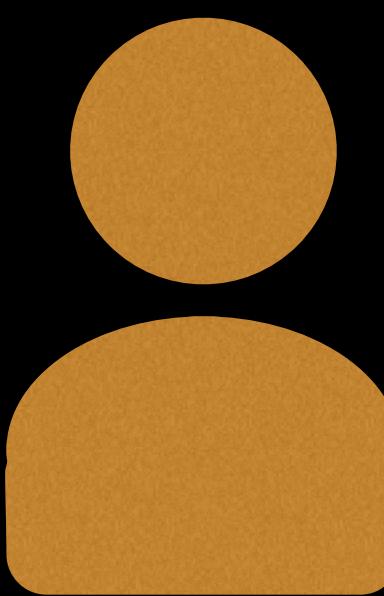
AVC

DAC

MAC

Policy Module

Policy Manager



SEACAT rule

SELinux rule

allow trusted_app my_file:file read_write

Domain

Type

Class

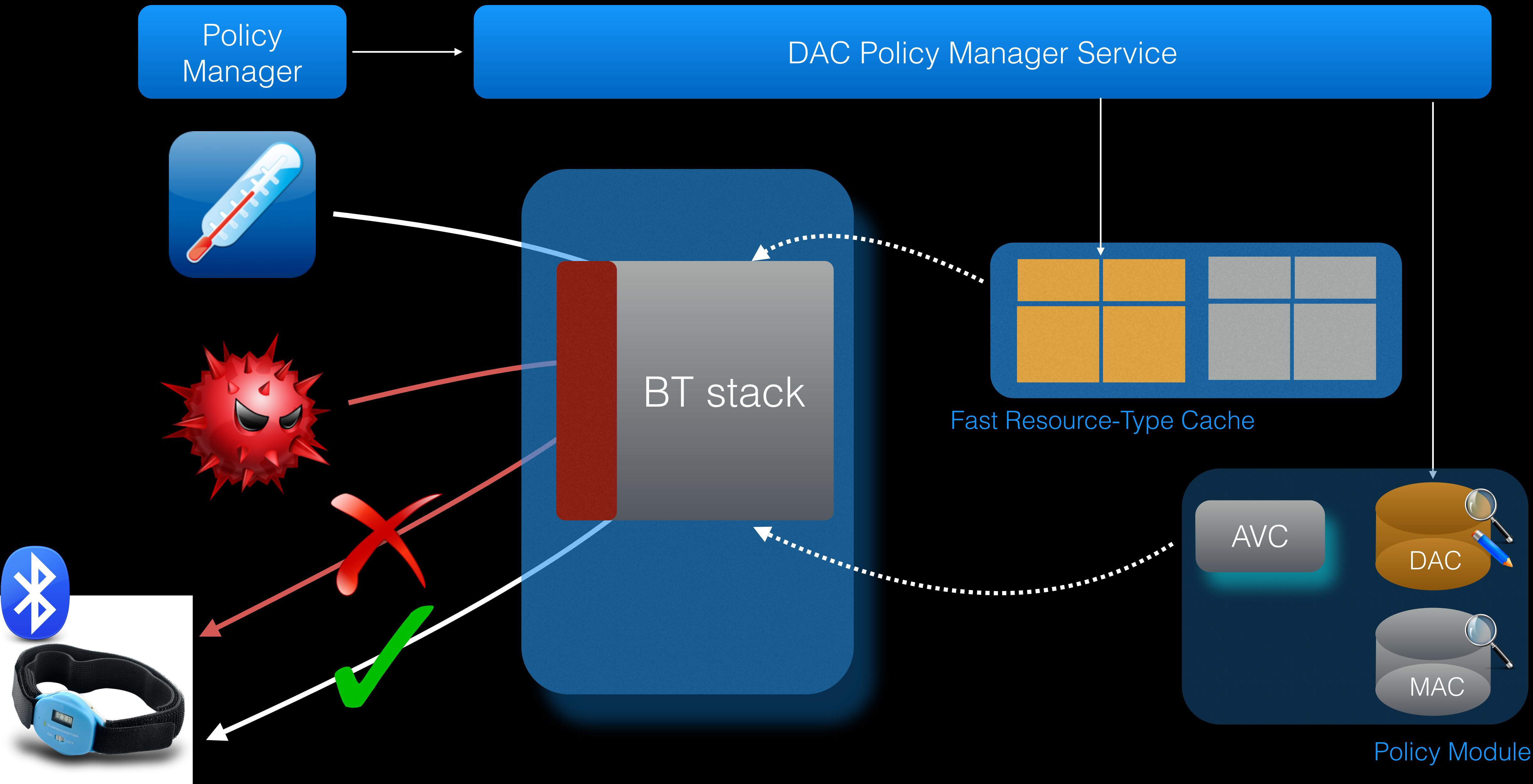
Access Vector

SEACAT rule

allow trusted_app bt_dev1:btacc connect

Enforcing the policies

SEACAT Enforcement



Evaluation

Effectiveness Evaluation

KNOWN THREATS

Bluetooth Mis-bonding attack ♦

Unauthorized adb-based screenshots ♦

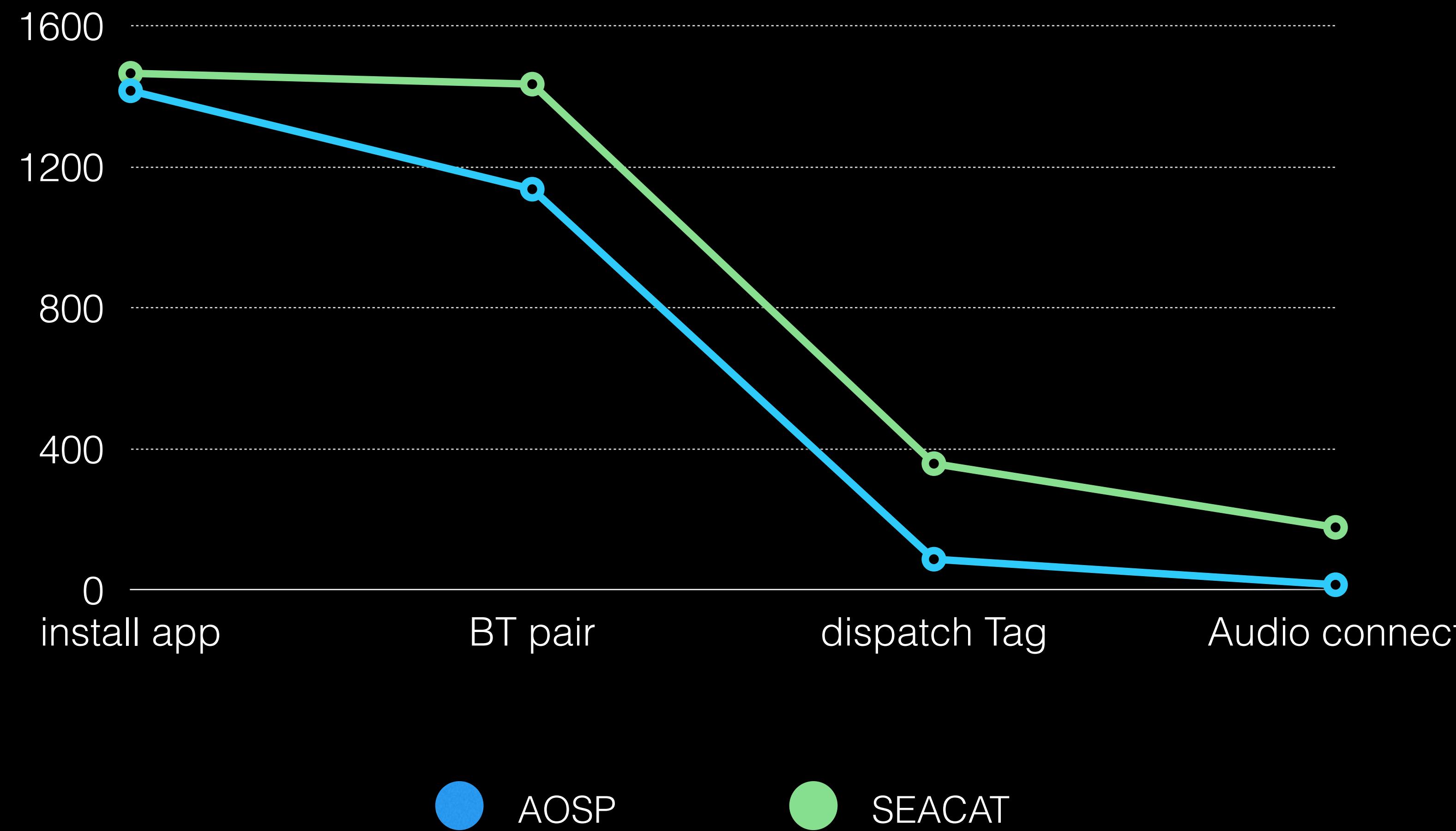
Unauthorized read of an SMS message

Unauthorized access to audio device

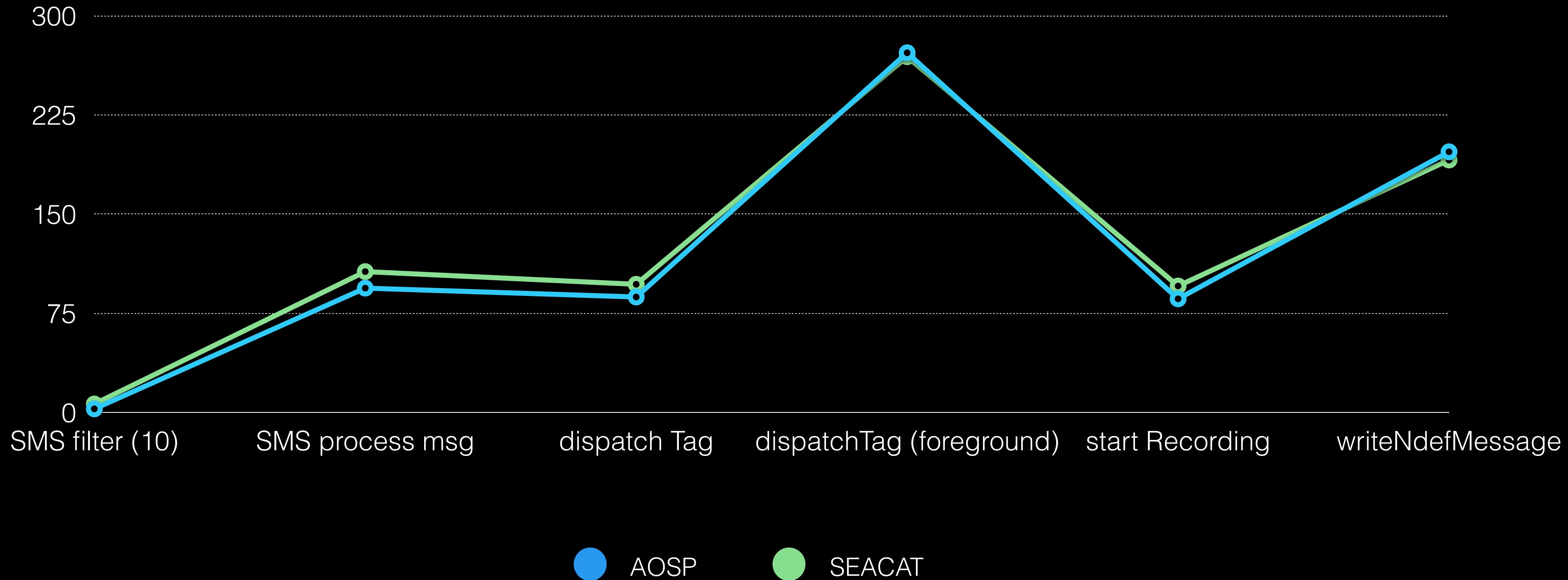
Unauthorized read of an NFC device's contents

♦ demonstrated in related work

Performance Evaluation (DAC Labeling)



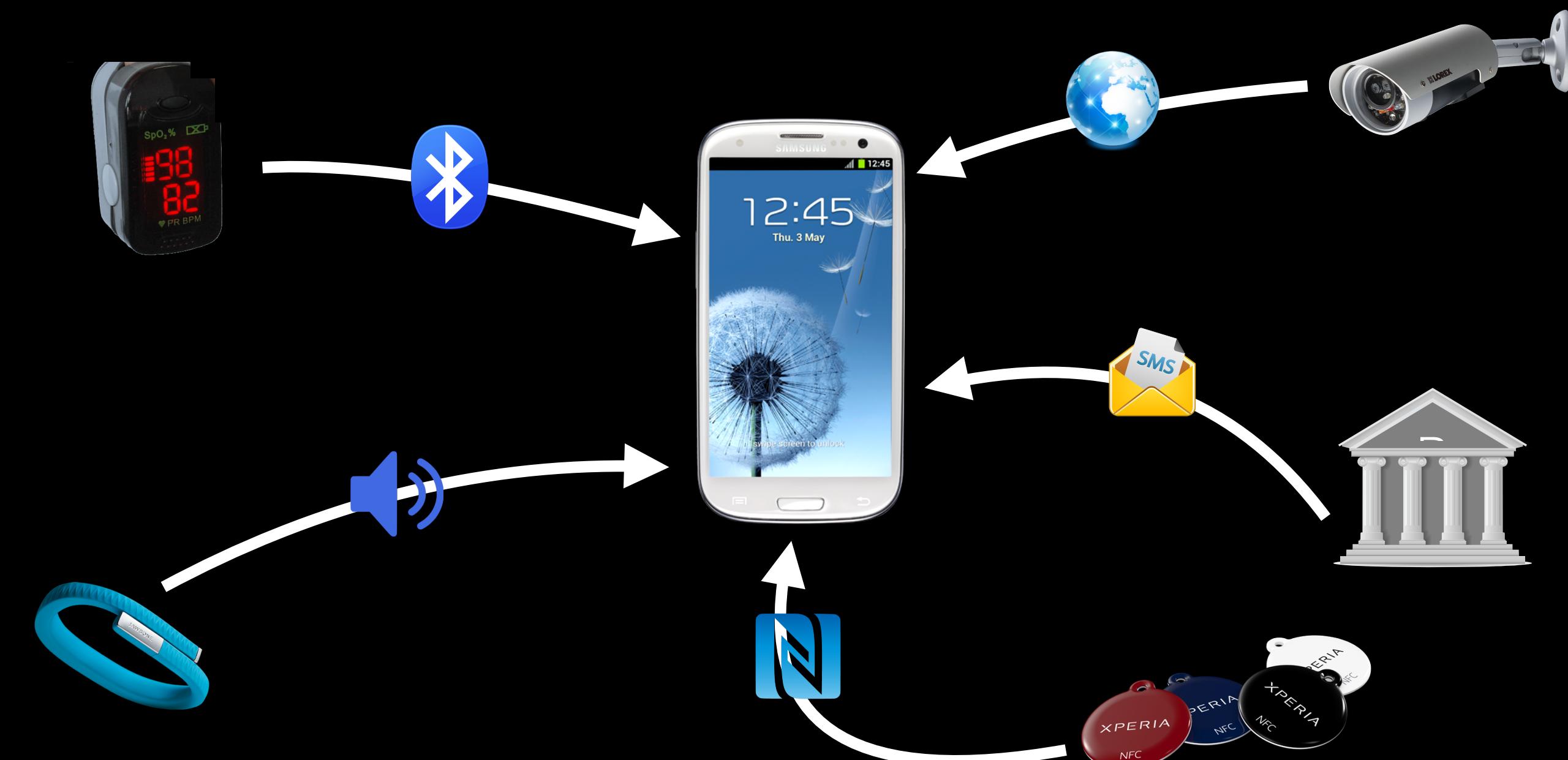
Performance Evaluation (enforcement)



Summary

Summary

Protection of Android external resources
MAC for vendors and admins
DAC for users
Backward compatible
Effective and efficient



Summary

- Protection of Android external resources
- MAC for vendors and admins
- DAC for users
- Backward compatible
- Effective and efficient



Thank You!

VIDEO DEMOS: [sites.google.com/
site/SeacatChannelControl](https://sites.google.com/site/seacatchannelcontrol)

